PATENT
Customer No. 22,852
Attorney Docket No. 07451.0029-00
Intertrust Ref. No.: IT-28.1 (US)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	)
Michael K. MACKAY et al.	) Group Art Unit: 2131
Application No. 09/653,517	) Examiner: Shin-Hon CHEN
Filed: August 31, 2000	) Confirmation No.: 4624
For: DATA PROTECTION SYSTEMS AND METHODS	)

MAIL STOP AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Applicants request a pre-appeal brief review of the Final Office Action dated June 1, 2006 ("Final Office Action"). This Request is being filed concurrently with a Notice of Appeal.

I. Requirements For Submitting a Pre-Appeal Brief Request for Review

Applicants have met each of the requirements for a pre-appeal brief review of rejections set forth in an Office Action. The application has been at least twice rejected. Applicants have filed a Notice of Appeal with this Request, and have not yet filed an Appeal Brief. Lastly, Applicants submit a Pre-Appeal Brief Request for Review that is five (5) or less pages in length and sets forth legal or factual deficiencies in the rejections. *See* Official Gazette Notice, July 12, 2005. Therefore, Applicants request review of the Examiner's rejections in the Final Office Action for the following reasons. Applicants reserve the right to raise additional arguments on appeal, including arguments that could have been raised here.

II. The Examiner's Rejection of Claims 1-3, 5, 7-9 and 14-20 Over Grecsek is Clearly Erroneous

The Examiner rejected claims 1-3, 5, 7-9, and 14-20 under 35 U.S.C. § 102(e) as allegedly anticipated by Grecsek. Claim 1 recites a step of "identifying one or more software modules responsible for processing the piece of electronic media content and

enabling use of the piece of electronic media content by the user; evaluating one or more predefined characteristics of the one or more software modules to determine..." In rejecting claim 1, the Examiner erred in finding that Grecsek teaches these elements.

Grecsek discloses a method for managing the risk of executing a software process on a computer. Grecsek is concerned with protecting the user's system from attacks by a process that will execute on the system. In order to manage the risk of executing a software process, the system disclosed in Grecsek evaluates the capabilities of the process against a capability-based policy. *See* Grecsek, col. 3, line 24 to col. 4, line 20. The capability-based policy includes a list of capabilities that may be allowed to be possessed by a process that is to be executed on the system. *Id.* If the capabilities possessed by the process are all present in the capability-based policy, the process may be permitted to execute on the system. *See* Grecsek, col. 4, lines 7-19. In Grecsek, prior to the evaluation, the process should not be authorized to execute on the system.

Claim 1 in the present application recites a method for protecting electronic media content from unauthorized use by a user of a computer system. In determining whether the computer system is operable to use the piece of electronic content in an authorized manner, one or more software modules that are responsible for processing the piece of electronic media content are identified. The system in Grecsek is used to evaluate whether a process (that may be new to the computer system) may cause undesirable effects on the computer system or the resources of the computer system. The process is probably brought by a user to execute on the computer system. The system in Grecsek does not identify "one or more software modules." There is no teaching of "identifying one or more software modules" that are "responsible for processing the piece of electronic media content ..." Therefore, claim 1 is distinguishable over Grecsek.

Furthermore, in Grecsek, the evaluation determines whether the process is allowed to execute on the computer system. Before the evaluation, the process is not allowed to execute on the computer system. Grecsek does not teach "evaluating one or more predefined characteristics of the one or more software modules to determine if the one or more software modules are operable to process the electronic media content in an authorized manner, ..." as recited in claim 1. These features further distinguish claim 1 from Grecsek.

Independent claim 5 is also directed to a method for protecting electronic media content from unauthorized use. The method includes a process of monitoring at least one system interface for electronic data, generating an identifier associated with the electronic data, comparing the identifier with an identifier associated with a piece of electronic media content. In the Final Office Action, the Examiner indicated column 4, lines 7-20, lines 28-37, and lines 50-55 of Grecsek as allegedly teaching these steps. Column 4, lines 7-20 teaches comparing capabilities of the process 110 to the capability list 210, and determining whether the process 110 is permitted to execute on the computer system. Column 4, lines 28-37 teaches a process of capabilities assessment. Column 4, lines 50-55 teaches that policy enforcer 117 stores modification detection codes, etc. None of the passages indicated by the Examiner teaches or suggests:

"monitoring at least one system interface for electronic data, the monitoring including:

receiving a piece of electronic data;

generating a second identifier associated with the piece of electronic data;

comparing the second identifier with the first identifier."

Therefore, Applicants respectfully submit that claim 5 is not anticipated by Grecsek.

Claims 2-3, and 6-20 are ultimately dependent from claims 1 or 5, respectively, and are thus allowable for at least the reasons set forth above in connection with claims 1 and 5. The deficiencies in Grecsek identified above are not cured by Davis, Ciacelli, or Shimada, the other art cited by the Examiner. Applicants therefore respectfully request that the Examiner withdraw the rejection of claims 1-3 and 5-20 and allow these claims.

III. The Examiner's Rejection of Claim 4 under 35 U.S.C. § 103(a) is Also Erroneous

Claim 4 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Grecsek in view of Davis.

Claim 4 is directed to a system for protecting electronic media content and enabling use of the electronic media content by a user. The Examiner indicated that Grecsek discloses all the limitations in claim 4 except "means for applying a cryptographic fingerprint to the electronic media content." While Applicants agree that Grecsek does not teach that limitation, Applicants also submit that Grecsek does not

teach "means for monitoring a predefined system interface for data containing the identifier," as is also recited in claim 4. The Examiner points to column 3, lines 35-50, of Grecsek as allegedly teaching this element. However, the cited passage (column 3, lines 35-50) states only that a computer system may have a policy containing a list of potential capabilities that process 110 may possess. Neither this passage, nor Davis as a whole, teaches or discloses "means for monitoring a predefined system interface for data containing the identifier." Applicants submit that claim 4 is not obvious over Grecsek in view of Davis for at least this reason.

IV. The Examiner Failed to Consider Applicants' Submission that There is No Motivation to Combine Greczek and Davis

Moreover, as noted in Applicants' Response filed November 28, 2005 at page 10, the Examiner's combination of Davis and Grecsek would violate the requirements of M.P.E.P. § 2143.01, as the combination would render each of the cited references unsatisfactory for its intended purpose. Grecsek describes systems and methods for identifying malicious software code before the code is executed on a computer system. Grecsek at Column 2, lines 40-45. The systems and methods described in Grecsek "provide a means for determining the capabilities of [a potentially malicious] process ... before it executes." *Id.* at lines 23-27. A process that is determined to include potentially dangerous operations can be denied access to system resources or have certain operations disabled. *See*, Column 4, lines 21-36. Applicants note that the Examiner failed to address this point in the Final Office Action stating only that the combination would have been obvious to one having ordinary skill. Final Office Action, ¶ 20, p. 8.

Applicants submit that one of ordinary skill in the art would not have any motivation to combine Davis with Grecsek without the use of prohibited hindsight, since the two references address different problems and operate on different types of data, an argument also previously presented in Applicants' Response filed November 28, 2005, at pages 10-11. Davis is concerned with copy protection; not preventing the execution of malicious operations. The methods and systems described by Grecsek are directed to evaluating program operations, and do not address securing data using an encryption-decryption scheme within a separate hardware device. Conversely, the encryption-decryption methods and systems described in Davis do not relate to identifying malicious code and preventing the execution of such code.

For these reasons, Applicants respectfully request that the Examiner withdraw the rejection of claim 4.

V. Conclusion

Because the Examiner's rejection of the pending claims includes legal and factual deficiencies, Applicants are entitled to a pre-appeal brief review of the Final Office Action. And based on the foregoing arguments, Applicants request that the rejection of these claims be withdrawn and the claims allowed.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: September 29, 2006

By: _____
Weiguo Chen
L.R. No. L0024

Finnegan Henderson Farabow
Garrett & Dunner L.L.P.
901 New York Ave., N.W.
Washington, D.C. 20001
Attorney direct (650) 849-6729